



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,104	11/29/2000	Dmitrii Loukianov	10559/383001/P10189	6820
20985	7590	04/27/2004	EXAMINER	
FISH & RICHARDSON, PC 12390 EL CAMINO REAL SAN DIEGO, CA 92130-2081			MOORTHY, ARAVIND K	
		ART UNIT		PAPER NUMBER
		2131		10
DATE MAILED: 04/27/2004				

Please find below and/or attached an Office communication concerning this application or proceeding.

>>

XG

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	09/727,104	LOUKIANOV ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Aravind K Moorthy	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 18 July 2002.  
 2a) This action is FINAL.                    2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-30 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-30 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 29 November 2000 is/are: a) accepted or b) objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                         |                                                                             |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____                                                |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____                                                             | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

1. Claims 1-30 are pending in the application.
2. Claims 1-30 have been rejected.

### *Specification*

#### Content of Specification

- (a) Title of the Invention: See 37 CFR 1.72(a) and MPEP § 606. The title of the invention should be placed at the top of the first page of the specification unless the title is provided in an application data sheet. The title of the invention should be brief but technically accurate and descriptive, preferably from two to seven words may not contain more than 500 characters.
- (b) Cross-References to Related Applications: See 37 CFR 1.78 and MPEP § 201.11.
- (c) Statement Regarding Federally Sponsored Research and Development: See MPEP § 310.
- (d) Incorporation-By-Reference Of Material Submitted On a Compact Disc: The specification is required to include an incorporation-by-reference of electronic documents that are to become part of the permanent United States Patent and Trademark Office records in the file of a patent application. See 37 CFR 1.52(e) and MPEP § 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text were permitted as electronic documents on compact discs beginning on September 8, 2000.

Or alternatively, Reference to a "Microfiche Appendix": See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.

- (e) Background of the Invention: See MPEP § 608.01(c). The specification should set forth the Background of the Invention in two parts:
  - (1) Field of the Invention: A statement of the field of art to which the invention pertains. This statement may include a paraphrasing of the applicable U.S. patent classification definitions of the subject matter of the claimed invention. This item may also be titled "Technical Field."
  - (2) Description of the Related Art including information disclosed under 37 CFR 1.97 and 37 CFR 1.98: A description of the related art known to the applicant and including, if applicable, references to specific related art and

problems involved in the prior art which are solved by the applicant's invention. This item may also be titled "Background Art."

- (f) Brief Summary of the Invention: See MPEP § 608.01(d). A brief summary or general statement of the invention as set forth in 37 CFR 1.73. The summary is separate and distinct from the abstract and is directed toward the invention rather than the disclosure as a whole. The summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). In chemical cases it should point out in general terms the utility of the invention. If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.
- (g) Brief Description of the Several Views of the Drawing(s): See MPEP § 608.01(f). A reference to and brief description of the drawing(s) as set forth in 37 CFR 1.74.
- (h) Detailed Description of the Invention: See MPEP § 608.01(g). A description of the preferred embodiment(s) of the invention as required in 37 CFR 1.71. The description should be as short and specific as is necessary to describe the invention adequately and accurately. Where elements or groups of elements, compounds, and processes, which are conventional and generally widely known in the field of the invention described and their exact nature or type is not necessary for an understanding and use of the invention by a person skilled in the art, they should not be described in detail. However, where particularly complicated subject matter is involved or where the elements, compounds, or processes may not be commonly or widely known in the field, the specification should refer to another patent or readily available publication which adequately describes the subject matter.
- (i) Claim or Claims: See 37 CFR 1.75 and MPEP § 608.01(m). The claim or claims must commence on separate sheet or electronic page (37 CFR 1.52(b)(3)). Where a claim sets forth a plurality of elements or steps, each element or step of the claim should be separated by a line indentation. There may be plural indentations to further segregate subcombinations or related steps. See 37 CFR 1.75 and MPEP § 608.01(i)-(p).
- (j) Abstract of the Disclosure: See MPEP § 608.01(f). A brief narrative of the disclosure as a whole in a single paragraph of 150 words or less commencing on a separate sheet following the claims. In an international application which has entered the national stage (37 CFR 1.491(b)), the applicant need not submit an abstract commencing on a separate sheet if an abstract was published with the international application under PCT Article 21. The abstract that appears on the cover page of the pamphlet published by the International Bureau (IB) of the

Art Unit: 2131

World Intellectual Property Organization (WIPO) is the abstract that will be used by the USPTO. See MPEP § 1893.03(e).

- (k) Sequence Listing. See 37 CFR 1.821-1.825 and MPEP §§ 2421-2431. The requirement for a sequence listing applies to all sequences disclosed in a given application, whether the sequences are claimed or not. See MPEP § 2421.02.

3. The specification is missing the brief summary of the invention.

*Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

**4. Claims 1-5, 7 and 8 are rejected under 35 U.S.C. 102(b) as being anticipated by Garcken et al U.S. Patent No. 5,745,571.**

As to claim 1, Garcken et al discloses a controller [column 1, lines 59-61]. Garcken et al discloses monitoring incoming cable modem transmissions for decryption keys. Garcken et al

discloses monitoring conditions when the decryption keys are received [column 17, lines 13-25].

Garcken et al discloses a register [column 5, lines 43-51]. Garcken et al discloses storing the decryption keys only when the conditions meet the specified criteria [column 17, lines 26-65].

As to claim 2, Garcken et al discloses that the cable modem includes a key processing element that causes the keys to be processed by software [column 5 line 43 to column 6 line 16].

As to claim 3, Garcken et al discloses that the cable modem is a host migrated cable modem in which a host PC processes the keys [column 10, lines 4-31].

As to claim 4, Garcken et al discloses that the register includes a write enable function, which allows information to be stored in the register only when the write enable function is in a specified condition [column 10, lines 32-62].

As to claim 5, Garcken et al discloses that the controller allows operation with decryption keys only when the decryption keys are stored in the register [column 17, lines 53-65].

As to claim 7, Garcken et al discloses that the register stores a plurality of decryption keys [column 5, lines 43-51]. Garcken et al discloses each decryption key being uniquely associated with a specified identification number indicative of services for which the decryption key is applicable [column 6, lines 18-42].

As to claim 8, Garcken et al discloses that the register further includes a write enable function, associated with each identification number, and which enables keys to be stored in the register associated with the write enable function only when the write enable function is in a specified state [column 7, lines 18-30].

**5. Claims 9, 10 and 12-14 are rejected under 35 U.S.C. 102(b) as being anticipated by Ganesan U.S. Patent No. 5,838,792.**

As to claim 9, Ganesan discloses monitoring an incoming cable stream for a decryption key. Ganesan discloses that if a decryption key is present, then decrypting the decryption key in a host PC that is associated with the cable modem, but separate from the cable modem [column 11 line 65 to column 12 line 2]. Ganesan discloses allowing the decryption key to be used for decrypting the cable stream, only when the decryption key has been received in a specified way, otherwise not allowing the decryption key to be used for decrypting the cable stream [column 14, lines 14-53].

As to claim 10, Ganesan discloses that the specified way includes that the decryption key was received over the cable medium [column 11 line 65 to column 12 line 2].

As to claim 12, Ganesan discloses that the specified way includes that the decryption key is stored in a specified register [column 14, lines 30-53].

As to claim 13, Ganesan discloses storing the decryption key in a specified register when the allowing determines that the decryption key has been received in the specified way [column 15, lines 10-41].

As to claim 14 Ganesan discloses allowing the decryption key to be used only when the decryption key is stored in the register [column 16, lines 6-28].

**6. Claims 22-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Candelore U.S. Patent No. 6,363,149 B1.**

As to claim 22, Candelore discloses a networked system of nodes [column 4, lines 7-34]. Candelore discloses that each node being uniquely controlled according to a unique identifier. Candelore discloses at least one secure controller. Candelore discloses the secure controller including a capability of providing permission to the nodes individually, according to the unique

identifier [column 6, lines 29-64]. Candelore discloses that each the node includes a secure event detection element capable of receiving an encryption key from the secure controller [column 7, lines 13-35]. Candelore discloses a memory, storing the encryption key only when specified conditions occur [column 9, lines 35-48].

As to claim 23, Candelore discloses that each the node is a cable modem [column 4, lines 7-34].

As to claim 24, Candelore discloses monitor, in a first unit, a data stream for incoming keys of a specified format. Candelore discloses sending the keys to another unit, other than the first unit, for decryption. Candelore discloses enabling use of the keys only when the keys are received from the data stream in a specified way [column 7, lines 13-35].

As to claim 25, Candelore discloses that the stream is a stream of cable modem information [column 4, lines 7-34].

As to claim 26, Candelore discloses that the keys are DES encryption keys [column 10, lines 29-32].

As to claim 27, Candelore discloses storing the keys in a specified location when they are received in the specified way [column 10, lines 33-42].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**7. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Garcken et al U.S. Patent No. 5,745,571 as applied to claim 1 above, and further in view of McBride U.S. Patent No. 6,292,899 B1.**

As to claim 6, Garcken et al does not teach that the register includes a key destroy function, which allows a decryption key stored in the register to be marked as an invalid key, and prevents the key from being used for subsequent operations.

McBride teaches a register that includes a key destroy function. McBride teaches that it a decryption key stored in the register to be marked as an invalid key. McBride teaches that it prevents the key from being used for subsequent operations [column 6, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Garcken et al so that the register would have included a key destroy function. The decryption key stored in the register would have been marked as an invalid key that would have prevented the key from being used for subsequent operations.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Garcken et al by the teaching of McBride because it prevents unauthorized users to have access to encrypted information [column 2, lines 25-29].

**8. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan U.S. Patent No. 5,838,792 as applied to claim 9 above, and further in view of Shimizu et al U.S. Patent No. 6,684,198 B1.**

As to claim 11, Ganesan does not teach that the specified way includes that the decryption key was received associated with a particular service ID.

Shimizu et al teaches decryption keys that are associated with a particular service ID [column 2, lines 48-56].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ganesan et al so that the decryption keys were associated with the service ID.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ganesan by the teaching of Shimizu et al because it prevents unauthorized copying of program data [column 1, lines 64-67].

**9. Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan U.S. Patent No. 5,838,792 as applied to claim 9 above, and further in view of Choquet et al U.S. Patent No. 6,684,198 B1.**

As to claims 15-17, Ganesan does not teach that the specified way includes requiring the decryption key to meet each of a plurality of specified rules. Ganesan does not teach that the specified rules include key writing to a decryption engine being normally disabled. Ganesan does not teach that at least one of the specified rules defines that the cable modem only receives messages on the cable that are addressed to the specified cable modem, and disregards messages which are addressed to other than specified cable modem.

Choquet et al teaches decryption keys to meet specified rules. Choquet et al teaches that the specified rules include key writing to a decryption engine being normally disabled. Choquet et al teaches that at least one of the specified rules defines that a modem only receives messages on the transmission medium that are addressed to the specified modem, and disregards messages that are addressed to other than specified modem [column 9, lines 33-50].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ganesan et al so that the decryption keys would have had to meet specified rules. The specified rules would have included key writing to a decryption engine that was normally disabled. The cable modem would have only received messages on the cable that are addressed to the specified cable modem, and disregarded messages that are addressed to other than specified cable modem.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Ganesan by the teaching of Choquet et al because it provides a messaging system that does not require the assignment of new system addresses and is immune to aliasing and false triggering [column 4, lines 6-17].

**10. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan U.S. Patent No. 5,838,792 and Choquet et al U.S. Patent No. 6,684,198 B1 as applied to claim 15 above, and further in view of Doyle et al U.S. Patent No. 6,438,550 B1.**

As to claim 18-20, the Ganesan-Choquet combination does not teach that at least one of the specified rules include that a specified service ID for specified key ring material causes key write capability to be enabled for the that specified service ID. The Ganesan-Choquet combination does not teach that an additional rule that disables key write for the service ID after

Art Unit: 2131

key ring material is written to a storage area associated with the service ID. The Ganesan-Choquet combination does not teach that an additional rule that disables key write for the service ID, for specified time after writing the key ring material.

Doyle et al teaches a specified service ID for specified key ring material causes key write capability to be enabled for the that specified service ID. Doyle et al teaches a rule that disables key write for the service ID after key ring material is written to a storage area associated with the service ID. Doyle et al teaches a rule that disables key write for the service ID, for specified time after writing the key ring material [column 9, lines 24-67].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ganesan-Choquet combination so that a specified service ID for specified key ring material caused key write capability to be enabled for the that specified service ID. There would have been a rule that disabled key write for the service ID after key ring material is written to a storage area associated with the service ID. There would have been a rule that disabled key write for the service ID, for specified time after writing the key ring material.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ganesan-Choquet combination by the teaching of Doyle et al because it allows client authentication to various servers and to allow access to configuration information for various software applications at whatever client computer a user may access [column 2, lines 17-21].

**11. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ganesan U.S. Patent No. 5,838,792 and Choquet et al U.S. Patent No. 6,684,198 B1 as applied to claim 15 above, and further in view of Lerner et al U.S. Patent No. 6,157,722.**

As to claim 21, the Ganesan-Choquet combination does not teach that at least one of the specified rules include that the cable modem receives key ring material, writes the key ring material, and then destroys the key ring material.

Lerner et al teaches at least one of the specified rules include that a modem receives key ring material, writes the key ring material, and then destroys the key ring material [column 9, lines 27-34].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ganesan-Choquet combination so that one of the specified rules included that a cable modem received key ring material, wrote the key ring material, and then destroyed the key ring material.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified the Ganesan-Choquet combination by the teaching of Lerner et al because it prevents unauthorized access to the content of the communications [column 2, lines 45-57].

**12. Claims 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore U.S. Patent No. 6,363,149 B1 as applied to claim 24 above, and further in view of McBride U.S. Patent No. 6,292,899 B1.**

As to claims 28-30, Candelore does not teach that the keys are enabled for use only when they are stored in the specified location. Candelore does not teach enabling writing only when specified conditions occur. Candelore does not teach enabling specified keys to be destroyed.

McBride teaches keys that are enabled for use only when they are stored in the specified location. McBride teaches enabling writing only when specified conditions occur [column 5, lines 40-67]. McBride teaches enabling specified keys to be destroyed [column 6, lines 41-45].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Candelore so that the keys can only be used when they are stored in the volatile key apparatus. Writing the keys to memory would have only took place when specified conditions occur. Specified keys would have been destroyed if unauthorized users were trying to intercept the decryption keys.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Candelore by the teaching of McBride because it prevents unauthorized users to have access to encrypted information [column 2, lines 25-29].

***Conclusion***

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy  
April 21, 2004

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100